AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method for detecting intrusions in a wireless network, comprising the steps of:

researching and defining normal network behavior with the intent of ascertaining user and temporal patterns;

researching potential sources of information that will lead to the detection and classification of potentially intrusive events;

establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events;

analyzing and evaluating the knowledge base to create an attack model; ~~and~~

utilizing the attack model to provide an adaptive response to intrusions in the wireless network; and

developing a recovery model to recover from an intrusion of the wireless network.

2. (Original) A method according to claim 1 which further includes augmenting the researching step by collecting real-world information concerning intrusive events and updating the knowledge base

3. (Canceled)

4. (Original) A method according to claim 1 wherein the wireless network is the Tactical Internet.

5. (Original) A method according to claim 1 wherein the wireless network is a Situation Assessment Data Link (SADL).

6. (Original) A method according to claim 1 wherein the wireless network is a tactical data link.

7. (Currently Amended) A method according to claim [[1]] 6 wherein the tactical data link is a Link-16 type tactical data link and its logical extensions.

8. (Currently Amended) A method according to claim [[1]] 6 wherein the tactical data link is a Link-11 type tactical data link and its logical extensions.

9. (Currently Amended) A method according to claim [[1]] 6 wherein the tactical data link is a Link-22 type tactical data link

10. (Original) A method according to claim 1 wherein the knowledge base includes data relating to suspicious events including passive eavesdropping, deception and denial of service.

11. (Original) A method according to claim 8 wherein the attack model is utilized to generate signatures of suspicious events.

12. (Original) A method according to claim 8 wherein the attack model is utilized to generate recommendations regarding the design of a wireless network.

13. (Original) A method for detecting intrusions in a wireless network, comprising the steps of:

researching and defining normal network behavior with the intent of ascertaining user and temporal patterns;

researching potential sources of information that will lead to the detection and classification of potentially intrusive events;

augmenting the researching step by collecting real-world information concerning intrusive events and updating the knowledge base;

establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events;

analyzing and evaluating the knowledge base to create an attack model;

utilizing the attack model to provide an adaptive response to intrusions in the wireless network; and

developing a recovery model to recover from an intrusion of the wireless network.

14. (Original) A method for detecting intrusions in the Tactical Internet, comprising the steps of:

researching and defining normal network behavior with the intent of ascertaining user and temporal patterns;

researching potential sources of information that will lead to the detection and classification of potentially intrusive events;

establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events, wherein the knowledge base includes data relating to suspicious events including passive eavesdropping, deception and denial of service;

augmenting the researching step by collecting real-world information concerning intrusive events and updating the knowledge base;

analyzing and evaluating the knowledge base to create an IW attack model;

utilizing the IW attack model to provide an adaptive response to intrusions in the Tactical Internet; and

developing a recovery model to recover from an intrusion of the Tactical Internet.

15. (Original) A method for detecting intrusions in a RF based tactical data link, comprising the steps of:

researching and defining normal network behavior with the intent of ascertaining user and temporal patterns;

researching potential sources of information that will lead to the detection and classification of potentially intrusive events;

establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events, wherein the knowledge base includes data relating to suspicious events including passive eavesdropping, deception and denial of service;

augmenting the researching step by collecting real-world information concerning intrusive events and updating the knowledge base;

analyzing and evaluating the knowledge base to create an IW attack model;

utilizing the IW attack model to provide an adaptive response to intrusions in the RF based tactical data link; and

developing a recovery model to recover from an intrusion of the RF based tactical data link.

16. (Previously Presented) The method of claim 1, wherein said attack model comprises an identification of a plurality of types of hostile events and associated manifestations of anamolous network events.

17. (Previously Presented) The method of claim 1 further including the steps of generating signatures from said attack model.

18. (Previously Presented) The method of claim 1, wherein said wireless network is an RF radio communication system.

19. (Previously Presented) The method of claim 1, wherein said anomolous network activity comprises network performance data.

20. (Currently Amended) ~~The method of claim 19, wherein said~~ A method for detecting intrusions in a wireless network, comprising the steps of:

researching and defining normal network behavior with the intent of ascertaining user and temporal patterns;

researching potential sources of information that will lead to the detection and classification of potentially intrusive events;

establishing a knowledge base of anomalous network activity, comprising network performance data that includes noise, loss of service, signal quality and traffic levels;

analyzing and evaluating the knowledge base to create an attack model; and

utilizing the attack model to provide an adaptive response to intrusions in the wireless network.

21. (Previously Presented) A method for detecting intrusions in a RF-based radio communication system, comprising the steps of:

establishing a knowledge base of anomalous activity for classifying potentially intrusive events, wherein the knowledge base includes data relating to suspicious events including passive eavesdropping, deception and denial of service;

analyzing and evaluating the knowledge base to create an attack model that comprises an identification of a plurality of types of hostile events and associated manifestations of anamolous network events;

utilizing the attack model to provide an adaptive response to intrusions in the RF-based radio communication system; and

developing a recovery model to recover from an intrusion of the RF-based radio communication system.

22. (Previously Presented) The method of claim 21 further including the steps of generating signatures from said attack model.

23. (Previously Presented) The method of claim 21, wherein said anomolous activity comprises performance data.

24. (Previously Presented) The method of claim 23, wherein said performance data includes noise, loss of service, signal quality and traffic levels.